AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

64. (previously presented) A method of storing a data set on a storage device carrying a file of random data comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

65. (previously presented) A method of operating a computer to store a data set on a storage device carrying a file of random data, the method comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

66. (currently amended) ~~A method according to~~The method according to claim 64 in which the step of selecting the first location for storing the file index comprises the step of selecting the first location as a start point of the file index.

67. (currently amended) ~~A method according to~~The method according to claim 64 ~~in which~~further including storing the encrypted file index ~~is stored directly~~ at the first location within the file of random data, by replacing a respective portion of the file of random data.

68. (currently amended) ~~A method according to~~The method according to claim 64 in which the file index is stored at the first location within the file of random data by processing ~~the~~ random data within the file of random data using the encrypted file index.

69. (currently amended) ~~A method according to~~The method according to claim 64 ~~in which~~further including storing the encrypted data set ~~is stored directly~~ at the second location within the file of random data, by replacing a respective portion of the file of random data.

70. (currently amended) ~~A method according to~~The method according to claim 64 in which the data set is stored at the second selected location in the file of random data by processing ~~the~~ random data within the file of random data using the encrypted data set.

71. (currently amended) ~~A method according to~~The method according to claim 64 which comprises ~~the~~ a step of using the user input passphrase for generating a key for encrypting the file index.

72. (currently amended) ~~A method according to~~The method according to claim 64 in which the passphrase is used for generating a key for encrypting the data set.

73. (currently amended) ~~A method according to~~The method according to claim 64 in which the passphrase is used in selecting the second location within the file of random data.

74. (currently amended) ~~A method according to~~The method according to claim 64 in which at least one of the first location within the file of random data, the second

location within the file of random data, a key for the file index and a key for the data set is determined by using at least one hash function to operate on the user input passphrase.

75. (currently amended) ~~A method according to~~The method according to claim 64 in which the passphrase is operated on once to produce an output which is used for determining at least two of the first location within the file of random data, the second location within the file of random data, a key for the file index and a key for the data set.

76. (currently amended) ~~A method according to~~The method according to claim 64 in which the passphrase is operated on a plurality of times, each operation generating an output for use in determining at least one of the first location within the file of random data, the second location within the file of random data, a key for the file index and a key for the data set.

77. (currently amended) ~~A method according to~~The method according to claim 64 in which ~~the same~~a common key is used for encrypting the ~~set of~~ data set and~~as is used~~ for encrypting the file index.

78. (currently amended) ~~A method according to~~The method according to claim 64 which comprises ~~the~~ a step of storing further sets of data using ~~the same~~said passphrase.

79. (currently amended) ~~A method according to~~The method according to claim 78 which is such that a respective location for each data set is selected, each data set is encrypted and stored at the respective location, and respective entries are added to the file index.

80. (currently amended) ~~A method according to~~The method according to claim 64, comprising ~~the~~ a step of storing further file indexes within the file of random data, each of which indexes is associated with a respective passphrase and each of which indexes is encrypted and is stored at a location selected in dependence on the respective passphrase.

81. (currently amended) ~~A method according to~~The method according to claim 80 in which respective encryption keys are generated from the respective passphrases and these respective keys are used for encrypting data sets which are associated with each file index.

82. (currently amended) ~~A method according to~~The method according to claim 80 comprising ~~the~~ a step of selecting the passphrase for, and hence location for, an additional file index ~~with in the~~ knowledge of ~~all of the existing~~the respective passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

83. (currently amended) ~~A method according to~~The method according to claim 80, in which, where there are a plurality of file indexes stored in the file of random data, the method comprises ~~the~~ a step of selecting a location for an additional data set ~~in the~~with knowledge of ~~all of the existing~~the respective passphrases corresponding to file indexes already stored in the file of random data such that collisions may be avoided.

84. (currently amended) ~~A method according to~~The method according to claim 80 comprising ~~the~~ a step of storing additional data sets using a passphrase whilst in ignorance of at least one other existing passphrase.

85. (currently amended) ~~A method according to~~The method according to claim 80 comprising ~~the~~ a step of storing data sets in a predetermined relationship to ~~the~~ a respective file index to help prevent collisions, for example data sets may be stored adjacent to ~~the~~ a respective file index, data sets may be stored substantially contiguously to ~~the~~ a respective file index, and data sets may be stored at locations close to but after ~~the~~ a respective file index.

86. (currently amended) ~~A method according to~~The method according to claim 64 comprising ~~the~~ a step of storing data on a storage device carrying a plurality of files of random data.

87. (currently amended) ~~A method according to~~The method according to claim 64 in which the file index comprises a message authentication code.

88. (currently amended) ~~A method according to~~The method according to claim 87 in which the file index comprises a message authentication code of all associated data sets so as to facilitate ~~the~~ detection of tampering.

89. (currently amended) ~~A method according to~~The method according to claim 87 in which the file index comprises a message authentication code of ~~the whole of~~ the file of random data in its entirety for use in detecting other usage of the file of random data.

90. (currently amended) ~~A method according to~~The method according to claim 64 comprising ~~the~~ a step of pre processing the data set prior to encryption.

91. (currently amended) ~~A method according to~~The method according to claim 64 comprising ~~the~~ a step of presenting a user with an indication of ~~the~~ a location within the file of random data that will be selected for the file index when using a predetermined passphrase.

92. (currently amended) ~~A method according to~~The method according to claim 91 comprising ~~the~~ a step of accepting user entered trial passphrases and

providing ~~the~~ a user with an indication of ~~the~~ a location within the file of random data that will be selected for the file index for each trial passphrase.

93. (currently amended) ~~A method according to~~The method according to claim 91 comprising ~~the~~ a further step of providing to ~~the~~ a user an indication of the regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by ~~the~~ a user.

94. (currently amended) ~~A method according to~~The method according to claim 64 comprising ~~the~~ a step of receiving an indication from a user of a location within the file of random data which ~~the~~ a user desires to use for a file index.

95. (currently amended) ~~A method according to~~The method according to claim 94 comprising the step of suggesting possible passphrases to a user in response to a user indicating a location within the file of random data which ~~the~~ a user desires to use for a file index.

96. (currently amended) ~~A method according to~~The method according to claim 94 comprising ~~the~~ steps of receiving a user input passphrase and suggesting a modified passphrase.

97. (currently amended) ~~A method according to~~The method according to claim 96 in which the modification of the passphrase is selected so as to at least one

of: move ~~the~~ a location at which ~~the~~ an associated index would be stored towards a desired location indicated by ~~the~~ a user and strengthen the passphrase.

98. (currently amended) ~~A method according to~~The method according to claim 64 comprising ~~the~~ a step of deleting a data set stored on a storage device.

99. (currently amended) ~~A method according to~~The method according to claim 98 comprising ~~the~~ a step of removing ~~the~~ a respective entry from the file index.

100. (currently amended) ~~A method according to~~The method according to claim 99 in which the ~~deleting~~ step of deleting a data set comprises ~~the~~ a step of overwriting the data set with random data as well as removing the entry from the file index.

101. (currently amended) ~~A method according to~~The method according to claim 98 comprising ~~the~~ a step of ~~reorganising~~ reorganizing data stored in association with a file index when at least one data set referenced in that file index is deleted.

102. (currently amended) ~~A method according to~~The method according to claim 100 in which the step of overwriting ~~step~~ the data set comprises ~~the~~ a step of using at least one random data and encrypted data stored in the file of random data for generating pseudo-random data for overwriting deleted files.

103. (currently amended) ~~A method according to~~The method according to claim 102 in which the method comprises ~~the~~ a step of using random numbers from the file of random data that would be overwritten when adding a data set to replace any pseudo-random values previously used elsewhere within the file of random data.

104. (currently amended) A storage device comprising at least one storage area storing ~~carrying~~ a file of random data ~~in which file of random data is stored~~with a file index and a data set being stored in the file of random data, wherein the file index is encrypted and is stored at a first location determined by a passphrase, the data set is encrypted and is stored at a second location and the file index comprises an entry in respect of the data set, the entry comprising an indication of the second location.

105. (currently amended) ~~A storage device according~~The storage device according to claim 104 carrying software for use in ~~the~~ storing and extraction of data sets in the file of random data.

106. (currently amended) ~~A storage device according~~The storage device according to claim 104 in which the passphrase has been used to generate a key for at least one of encrypting the file index and encrypting the data set.

107. (currently amended) ~~A storage device according~~The storage device according to claim 104 in which ~~the~~ software carried by the storage device ~~is arranged~~

~~such~~comprises instructions that when loaded and run by a computer, cause the computer ~~is caused~~ to carry out at least one of the following steps:

accepting passphrases, generating corresponding keys, and determining respective locations for storage of file indexes;

encrypting file indexes;

encrypting data sets;

storing file indexes;

selecting locations for data sets;

storing data sets;

accepting passphrases and locating and decrypting respective file indexes;

locating and decrypting data sets;

retrieving data sets.

108. (currently amended) ~~A storage device according~~The storage device according to claim 104 which further carries a conventional file allocation table.

109. (currently amended) ~~A storage device according~~The storage device according to claim 104 which comprises a portion of Read Only Memory (ROM).

110. (currently amended) ~~A storage device according~~The storage device according to claim 108 which comprises a ROM portion that carries the file allocation table, ~~the~~ software and an operating system header file for the file of random data.

111. (previously presented) The storage device according to claim 104 which is a removable storage device.

112. (currently amended) ~~A storage device according~~The storage device according to claim 104 having a unique serial number.

113. (currently amended) ~~A storage device according~~The storage device according to claim 104 which carries a unique hard coded identifier which is used in at least one of:

a) ~~the~~ an encryption process used for encrypting at least one of the file index and the data; and

b) a decryption process used for decrypting at least one of the file index and the data.

114. (currently amended) ~~A storage device according~~The storage device according to claim 104 which is sold with a pretext for at least one use.

115. (currently amended) A computer arranged under the control of software, said computer executing instructions for storing a data set on a storage device carrying a file of random data, said computer ~~using~~performing ~~the~~ steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for ~~the~~ storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

116. (currently amended) ~~A computer according to~~The computer according to claim 115 which is arranged under the control of software to present a user with an indication of ~~the~~ a location within the file of random data that will be selected for storing the file index when using a predetermined passphrase.

117. (currently amended) ~~A computer according to~~The computer according to claim 115 which is arranged under the control of software to accept user entered trial passphrases and provide ~~the~~ a user with an indication of ~~the~~ a location within the file of random data that will be selected for storing the file index for each trial passphrase.

118. (currently amended) ~~A computer according to~~The computer according to claim 115 which is arranged under the control of software to provide ~~the~~ a

user an indication of ~~the~~ regions of the file of random data that are already occupied by file indexes having passphrases that have been supplied by ~~the~~ a user.

119. (currently amended) ~~A computer according to~~The computer according to claim 115 which is arranged under the control of software to suggest possible passphrases to a user in response to a user indicating a location within the file of random data which ~~the~~ a user desires to use for storing a file index.

120. (currently amended) ~~A computer according to~~The computer according to claim 116 which is arranged under the control of software to present a user interface for displaying the indications.

121. (currently amended) ~~A computer according to~~The computer according to claim 120 in which the user interface is arranged so that a user can use a pointing device to indicate ~~the~~ a location within the file of random data which ~~the~~ a user desires to use for storing a file index.

122. (currently amended) A method of extracting a data set stored on a storage device ~~according to claim 104~~carrying a file of random data with a file index and a data set being stored in the file of random data, wherein the file index is encrypted and is stored at a first location determined by a passphrase, the data set is encrypted and is stored at a second location and the file index comprises an entry in respect of the

data set, the entry comprising an indication of the second location, the method of extracting data comprising the steps of:

accepting a user input passphrase;

determining ~~the~~ a location for a file index indicated by the passphrase;

decrypting the file index;

identifying ~~the~~ a location of ~~the~~ a requested data set from the file index; and

decrypting the data set.

123. (currently amended) A computer arranged under the control of software to extract data using ~~a method according to~~The method according to claim 122.

124. (currently amended) A method of storing a data set on a storage device carrying a file of random data comprising the steps of:

selecting, in dependence on a user input passphrase, a first location within the file of random data for storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry made in the file index comprising a indication of the second selected location;

encrypting the file index; and

storing the file index at the first selected location in the file of random data,

wherein the method comprises the further steps, prior to ~~finalising~~ finalizing the user input passphrase, of accepting at least one user entered trial passphrase and providing ~~the~~ a user with an indication of ~~the~~ a location within the file of random data that will be selected for the file index associated with the at least one user entered trial passphrase.

125. (currently amended) A computer readable data carrier, carrying a computer program comprising code portions which when loaded and run on a computer cause the computer to carry out ~~a method according to claim 64~~ the following steps:

selecting, in dependence on a user input passphrase, a first location within the file of random data for storing a file index;

selecting a second location within the file of random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the file of random data;

making an entry in the file index in respect of the data set, the entry comprising an indication of the second selected location;

encrypting the file index; and

storing the encrypted file index at the first selected location in the file of random data.

126. (new) A method of storing a data set on a storage device having a data storage area initialized with random data comprising the steps of:

selecting a first location within the data storage area initialized with random data for storing a file index;

selecting a second location within the data storage area initialized with random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the data storage area

initialized with random data;

ensuring that an indication of the second selected location is determinable from the file index;

encrypting the file index; and

storing the encrypted file index at the first selected location in the data storage area initialized with random data, and comprising, before the step of encrypting the file index, a further step of recording in the file index an indication of which parts of the data storage area initialized with random data will be used to store said data set.

127. (new) The method according to claim 126 wherein the step of ensuring that an indication of the second selected location is determinable from the file index comprises the step of

making an entry in the file index in respect of the data set, the entry comprising an

indication of the second selected location.

128. (new) The method according to claim 126 wherein the step of selecting a first location within the data storage area initialized with random data for storing a file index, comprises

the step of selecting the first location from a plurality of predetermined possible locations within the data storage area initialized with random data, in dependence on

one of: an input received from a user; and a selection process which is independent of

user input.

129. (new) The method according to claim 126 wherein the step of selecting a first location within

the data storage area initialized with random data for storing a file, comprises steps of

selecting the first location in dependence on a user input passphrase and associating

the file index with the user input passphrase.

130. (new) The method according to claim 129 wherein said data set is stored under protection of

said user input passphrase and the method comprising a further step of storing a second data set on the storage device under protection of a second user input passphrase, the step of storing the second data set on the storage device comprising

steps of:

selecting, in dependence on the second user input passphrase, a third location within

the data storage area initialized with random data for storing a second file index;

selecting a fourth location within the data storage area initialized with random data for

storing the second data set;

encrypting the second data set;

storing the encrypted second data set at the fourth selected location in the data storage

area initialized with random data;

ensuring that an indication of the fourth selected location is determinable from the

second file index;

encrypting the second file index; and

storing the encrypted second file index at the third selected location in the data storage

area initialized with random data, and comprising, before the step of encrypting the

second file index, a further step of recording in the second file index an indication of

which parts of the data storage area initialized with random data will be used to store

said second data set.

131. (new) The method according to claim 126 wherein the data storage area initialized with random data is reserved for use in storing data.

132. (new) The method according to claim 126 wherein the data storage area initialized with random data comprises a file of random data which is managed by a conventional file system on a computer.

133. (new) A removable storage device comprising a data storage area initialized with random data, wherein a file index and a data set are stored in the data storage area initialized with random data, the file index is encrypted and stored at a first location within the data storage area initialized with random data, the data set is encrypted and stored at a second location within the data storage area initialized with random data, the file index comprises an entry in respect of the data set, the entry comprising an indication of the second location within the data storage area initialized with random data, and the file index comprises an indication of which parts of the data storage area initialized with random data are in use to store said data set.

134. (new) A removable storage device carrying software and comprising a data storage area initialized with random data, the software comprising code portions which when loaded and run on a computer cause the computer to execute a method of storing a data set on the storage device, the method comprising the steps of:

selecting a first location within the data storage area initialized with random data for storing a file index;

selecting a second location within the data storage area initialized with random data for storing the data set;

encrypting the data set;

storing the encrypted data set at the second selected location in the data storage area initialized with random data;

ensuring that an indication of the second selected location is determinable from the file index;

encrypting the file index; and

storing the encrypted file index at the first selected location in the data storage are initialized with random data, and comprising, before the step of encrypting the file index, a further step of recording in the file index an indication of which parts of the data storage area initialized with random data will be used to store said data set.